Security Confidence Test - EGS7

Test Objectives:

The objectives of this test are to verify the security functions of the EGS. These functions include:

- user access to secure data,
- the ability to prevent deliberate or unintentional corruption of data,
- virus detection,
- audit trailing,
- the systems response to security compromises,
- recovery from security violations, and
- security safeguards.

Test Configuration:

Hardware and software configurations at each ECS site are managed and tracked by the M&O organization at that site. The most current configuration status report will be obtained prior to the start of testing and be referenced in the test report.

Participants and Support Requirements:

Participants:

M&O Support at the DAACs

Communications:

Voice - N/A
Data - N/A
IP address: N/A

Equipment and Software:

Hardware: The LSM is responsible for the security of the system.
Software: Kerberos, DCE, and Tivoli

Test Tools:

ISS for internet connections verification
SATAN for user access verification

Test Data:

Description / Characteristics	Source	File/script name & Location
Data with limited access	DAACs	
Computer Virus	I&T team	

Test Case Descriptions:

EGS7.1 Data Access

This test verifies that users cannot access restricted data unless they have access privileges. A privileged user updates restricted data while an unprivileged user is refused access. Group passwords are also verified in this test. Web access is demonstrated and verified.

Requirements to be Verified:

EOSD2550#A	The ECS elements shall limit use of master passwords or use of a single password for large organizations requiring access to a mix of security controlled and non-sensitive data.
ESN-1400#A	The following security functions and services, at a minimum, shall be provided:a. authenticationb. access (authorization) controlc. data integrityd. data confidentiality
IMS-0060#A	The IMS shall, when creating ECS user accounts, request registration approval, user account priorities, and authorized user services from the SMC.
IMS-0230#A	The IMS shall restrict update of ECS directory, inventory, and guide documentation/reference material) and other IMS data bases to authorized users based on the users access privileges.
SMC-5320#A	The SMC shall establish, maintain, and authenticate access privileges for ECS scientific users.
SMC-5325#A	The LSM shall promulgate, maintain, authenticate, and monitor user and device accesses and privileges.
SMC-5330#A	The SMC shall provide support, manage, maintain, and request security testing that includes, at a minimum, password checking and control of site and element internal privileges.
SMC-5335#A	The LSM shall perform security testing that includes, at a minimum, password auditing and element internal access/privileges checking.
SMC-7300#A	The SMC shall establish, maintain, and update the authorized users inventory to include, at a minimum: a. Users identifications b. Addresses c. Allowed privileges

EGS7.2 Virus Detection

This test verifies that the ECS detects attempts to ingest information which contains virus and/or worms. A user logs into the system using a PC. While logged onto the system, the user attempts to push a document onto the system which contains a virus. The system should detect the virus and alert system personnel. A virus is also attached to a mail message and attempt to enter the system. The system should detect the corrupt attachment and alert the operators.

Requirements to be Verified:

EOSD2510#A	ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms g. Actions taken to contain or destroy a virus
SMC-5345#A	The LSM shall perform compromise (e.g., virus or worm penetration) risk analysis, and detection.

EGS7.3 System Recovery

This test verifies that the system can recover from a system failure due to 1) a loss in the integrity of the data and 2) catastrophic violation of the security system. An attempt to breach the system security is monitored to test the systems ability to detect and respond to the violation.

Requirements to be Verified:

EOSD2510#A	ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms g. Actions taken to contain or destroy a virus
EOSD2990#A	The ECS elements shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security system.
ESN-1380#A	The ESN shall provide countermeasures for the following security threats related to data communications:a. modification of data (i.e., manipulation) while in transit over the networkb. disclosure of authentication informationc. degradation in network or processing resource performance through denial of service attack d. Impersonation of authentication credentials or authorization privileges.
SMC-0350#A	The SMC shall have the capability of responding to security compromises within a maximum of five minutes.
SMC-5330#A	The SMC shall provide support, manage, maintain, and request security testing that includes, at a minimum, password checking and control of site and element internal privileges.
SMC-5335#A	The LSM shall perform security testing that includes, at a minimum, password auditing and element internal access/privileges checking.
SMC-5365#A	The LSM shall generate recovery actions in response to the detection of compromises.
SMC-8880#A	The SMC shall have the capability to generate detailed and summary security compromise reports indicating security compromises of ground resources and facilities, including, at a minimum:a. Security compromise type and descriptionb. Time of occurrencec. Cause of security compromised. Impact on systeme. Status of security compromise resolutionf. Security compromise statisticsg. Results of security compromise risk analysis

EGS7.4 Audit Trials

This test verifies that all the information required for the audit trails is being maintained. Reports are generated and content verified. System backups are verified to include audit trails. Security policies and procedures are also verified.

Requirements to be Verified:

EOSD2510#A	ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms g. Actions taken to contain or destroy a virus
EOSD3200#A	A minimum of one backup which is maintained in a separate physical location (i.e., different building) shall be maintained for ECS software and key data items (including security audit trails and logs).
ESN-0650#A	The ESN shall perform the following network management functions for each protocol stack implemented in any ECS element, and each communications facility:a. Network Configuration Managementb. Network Fault Managementc. Network Performance Managementd. Network Security Management
ESN-1430#A	The ESN shall provide the following security event functions: a. Event detection b. Event reporting c. Event logging
SMC-5305#A	The LSM shall maintain security policies and procedures, including, at a minimum:a. Physical securityb. Password managementc. Operational securityd. Data classificationse. Access/privilegesf. Compromise mitigation
SMC-5340#A	The SMC shall perform security risk analyses and compromise detection.
SMC-5345#A	The LSM shall perform compromise (e.g., virus or worm penetration) risk analysis, and detection.
SMC-8880#A	The SMC shall have the capability to generate detailed and summary security compromise reports indicating security compromises of ground resources and facilities, including, at a minimum:a. Security compromise type and descriptionb. Time of occurrencec. Cause of security compromised. Impact on systeme. Status of security compromise resolutionf. Security compromise statisticsg. Results of security compromise risk analysis

EGS7.5 Unscheduled System Shutdown

This test demonstrates the systems ability to respond to an unscheduled system shutdown (such as a power outage or system abort) and the ability of the system to be restarted from this state. Functions in progress (i.e. data ingest, data archive, data producton) should be restarted automatically or reported as incomplete.

Requirements to be Verified:

EOSD2440#A	Data base integrity including prevention of data loss and corruption shall be maintained.
EOSD3000#A	The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup.

EGS07.6 FOS Specific Security Test

This test verifies specific security functionality that is unique to the FOS.

Requirements to be Verified:

Requirement	Description	Test Cases
EOSD2430#A ***Partial***	Data base access and manipulation shall accommodate control of user access and update of security controlled data.	EGS07.6
EOSD2440#A	Data base integrity including prevention of data loss and corruption shall be maintained.	EGS07.6
EOSD2510#A ***Partial***	ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms g. Actions taken to contain or destroy a virus	EGS07.6
EOSD2550#A ***Partial***	The ECS elements shall limit use of master passwords or use of a single password for large organizations requiring access to a mix of security controlled and non-sensitive data.	EGS07.6
EOSD2990#A ***Partial***	The ECS elements shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security system.	EGS07.6
EOSD3000#A ***Partial***	The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup.	EGS07.6
EOSD3200#A	A minimum of one backup which is maintained in a separate physical location (i.e., different building) shall be maintained for ECS software and key data items (including security audit trails and logs).	EGS07.6
EOSD3220#A	All media shall be handled and stored in protected areas with environmental and accounting procedures applied.	EGS07.6

EGS7.7 EOSDIS\ASTER Security

The objective of this test is to verify the user authentication of both ASTER GDS users for the EOSDIS privileges and EOSDIS users for ASTER GDS privileges.

Requirements to be Verified:

ASTER-0880	ECS shall have the capability to send and ASTER GDS shall have the capability to receive user authentication requests for ASTER GDS privileges of EOSDIS users.
ASTER-0885	ASTER GDS shall have the capability to send and ECS shall have the capability to receive user authentication information specifying ASTER GDS privileges for EOSDIS users.
ASTER-0890	ASTER GDS shall have the capability to send and ECS shall have the capability to receive user authentication requests for ECS privileges of ASTER GDS users.
ASTER-0895	ECS shall have the capability to send and ASTER GDS shall have the capability to receive user authentication information specifying ECS privileges for ASTER GDS users.
ASTER-1080	The interface between ECS and ASTER GDS shall be compliant with the interface guidelines

	identified in the ECS Security plan

Test Procedures:

Test Set-up
EGS7.6 FOS Specific Security Test

Step	Station	Action	Expected Results	Comments
1.	EOC	Acquire account name/password with Command Activity Controller (CAC) priveleges.		
2.	EOC	Record the system configuration on the execution cover sheet		
3.				
4.				
5.		Request Command Activity Controller (CAC) privilege. TAKE COMMAND STRING = 100		
6.	EOC	Bring up event page		
7.				

Test Execution:
EGS7.6 FOS Specific Security Test

Step	Station	Action	Expected Results	Comments
1.	EOC	Attempt to login to FOS system using invalid username and acceptable password.	Access denied	
2.	EOC	Attempt to login to FOS system using valid username and invalid password.	Access denied	
3.	EOC	Repeat the attempted login process with the **same valid username** and **different invalid passwords** until the system shuts out the user's attempt to login.	Number of attempts required: _____	
4.	EOC	System Administrator reset account.		
5.	EOC	Attempt to login to FOS system using valid username and invalid password.	Access denied	
6.	EOC	Repeat the attempted login process with **different valid usernames** and **invalid passwords** until the system shuts out the user's attempt to login.	Usernames used: _____ _____ _____	
7.	EOC	System Administrator reset accounts/workstation.		

Step	Station	Action	Expected Results	Comments
8.	~	Two FOS users login at EOC workstations and initialize necessary subsystems. One user has privelges to access and manipulate the FOS databases and the other does not.		
9.	EOC	Login to the FOS system using valid username and valid password.	Access to system granted.	
10.	EOC	Initialize necessary subsystems Start the **A2_UserStationStartup** shell script.	FOS logical string is configured for test execution.	AM-1 GSCID: (CTIU-1)=A9 000010101001 (CTIU-2)=AA 000010101010
11.	EOC	A second user, without privelges to access and manipulate the FOS databases, login to the FOS system.	Access to system granted.	
12.	EOC	A second user initialize necessary subsystems Start the **A2_UserStationStartup** shell script.	FOS logical string is configured for test execution.	
13.	~	Data base access and manipulation shall accommodate control of user access and update of security controlled data.		EOSD2430#A
14.	~	Data base integrity including prevention of data loss and corruption shall be maintained.		EOSD2440#A
15.	~	ECS elements shall maintain an audit trail of: a. All accesses to the element security controlled data b. Users/processes/elements requesting access to element security controlled data c. Data access/manipulation operations performed on security controlled data d. Date and time of access to security controlled data e. Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes f. Detected computer system viruses and worms g. Actions taken to contain or destroy a virus		EOSD2510#A
16.	EOC	Attempt to access FOS security controlled data by a user who is not authorized.	Data and location TBD.	

Step	Station	Action	Expected Results	Comments
17.	EOC	A second unauthorized user will attempt to access FOS security controlled data		
18.	EOC	Access FOS security controlled data by an authorized user.		
19.	EOC	Manipulate the security controlled data.		
20.	EOC	Review the audit trail of: All accesses to the element security controlled data	Audit trail exists, is current, accurate, and complete.	Identify FOS security controlled data
21.	EOC	Review the audit trail of: Users/processes/elements requesting access to element security controlled data	Audit trail exists, is current, accurate, and complete.	
22.	EOC	Review the audit trail of: Data access/manipulation operations performed on security controlled data	Audit trail exists, is current, accurate, and complete.	
23.	EOC	Review the audit trail of: Date and time of access to security controlled data	Audit trail exists, is current, accurate, and complete.	
24.	EOC	Review the audit trail of: Unsuccessful access attempt to the element security controlled data by unauthorized users/elements/processes	Audit trail exists, is current, accurate, and complete.	
25.	EOC	Introduce a simulated or benign virus into the FOS system.	Panic, paranoia, mayhem	At least ftp a file that contains a virus, but do not execute or access it.
26.	EOC	Introduce a simulated or benign worm into the FOS system.		Perhaps a self-destructing worm?
27.	EOC	Observe the operation of virus and worm detecting processes.	Virus and worm detected, located, and operator notified.	
28.	EOC	Observe the virus and worm are permanently destroyed.		
29.	EOC	Review the audit trail of: Detected computer system viruses and worms	Audit trail exists, is current, accurate, and complete.	
30.	EOC	Review the audit trail of: Actions taken to contain or destroy a virus	Audit trail exists, is current, accurate, and complete.	
31.	~	The ECS elements shall limit use of master passwords or use of a single password for large organizations requiring access to a mix of security controlled and non-sensitive data.		EOSD2550#A
32.	EOC	Review password policy in effect, and policy manual.		Is policy adequate?

Step	Station	Action	Expected Results	Comments
33.	EOC	Get a warm fuzzy that password policy is being, and will continue to be, adhered to.		
34.	~	The ECS elements shall support the recovery from a system failure due to a loss in the integrity of the ECS data or a catastrophic violation of the security system.		EOSD2990#A
35.	~	The ECS shall provide for security safeguards to cover unscheduled system shutdown (aborts) and subsequent restarts, as well as for scheduled system shutdown and operational startup.		EOSD3000#A
36.	~	A minimum of one backup which is maintained in a separate physical location (i.e., different building) shall be maintained for ECS software and key data items (including security audit trails and logs).		EOSD3200#A
37.	EOC	Verify that a FOS software backup is being maintained at a separate physical location.	Location: _____ Data: _____ Frequency of update at this location _____ Person responsible: _____	
38.	EOC	Verify that FOS security audit trails and logs are being maintained at a separate physical location.	Location: _____ Data: _____ Frequency of update at this location _____ Person responsible: _____	
39.	EOC	Verify that other FOS key data items are being maintained at a separate physical location.	TBD	
40.	~	All media shall be handled and stored in protected areas with environmental and accounting procedures applied.		EOSD3220#A
41.				

Test Termination:
EGS7.6 FOS Specific Security Test

Step	Station	Action	Expected Results	Comments
1.	EOC	Collect all necessary screen snaps, dumps, etc. needed for post-test analysis and verification		
2.	EOC	Reconfigure the system to pre-test configuration		

Step	Station	Action	Expected Results	Comments
3.	EOC	Log off of the FOS user workstations. Execute the **MyKill** script (Rls A only).		